

NAVPGSCOLINST 5230.4C  
NPS (05)  
17 Aug 00

NAVPGSCOL INSTRUCTION 5230.4C

Subj: POLICY ON APPROPRIATE USE OF NAVAL POSTGRADUATE SCHOOL  
COMPUTING AND INFORMATION SYSTEMS

Ref: (a) Department of Defense (DoD) Web Site Administration  
Policies and Procedures  
(b) OPNAVINST 5300.8B  
(c) Department of Defense (DoD) Instruction 1100.13,  
Surveys of DoD Personnel  
(d) SECNAVINST 5720.47

1. Purpose. To establish general Naval Postgraduate School (NPS) policy on appropriate use of NPS computing and information systems, and standards of conduct for users of those systems, consistent with the NPS mission and Department of the Navy/Department of Defense (DON/DoD) guidelines.

2. Cancellation. NAVPGSCOLINST 5230.4B

3. Applicability. This instruction applies to all users of computer and information systems owned or operated by NPS, its tenant commands and activities. It also applies to users of any computer or information system, regardless of ownership, that is either remotely or directly connected to the NPS network.

4. Background

a. The principal mission of NPS is graduate education. To properly execute this mission, NPS must support the intellectual and professional growth of its faculty, staff and students. NPS is also a military command within DON/DoD and must, therefore, operate under Federal and DoD guidelines. These guidelines specify that Government resources, including computer and information systems, may be used for authorized, "official" purposes, only.

b. The expanded use of the Internet, electronic mail, and web technology provide the individual user an almost unlimited capability for communication and rapid access to, and transfer of information. In taking full advantage of the opportunities

that these technologies provide, the boundaries between appropriate (official) and inappropriate uses can frequently become blurred. The need to clarify these boundaries requires that NPS define clear and explicit policies on appropriate and acceptable use of its computer and information systems.

## 5. Policy

a. In consideration of its primary educational mission, NPS authorizes use of its computing and information system resources for all purposes reasonably related to graduate education and research; to intellectual and scholarly inquiry; to the NPS military mission; and to the general professional interests and growth of its faculty, staff, and students. Faculty, staff, and students are encouraged to make maximum use of these resources for expanding their professional horizons, and for increasing their knowledge, skills, and ability to contribute to NPS and to the community at large. Minimal incidental and innocuous use of these resources for personal study and communications that contribute to generally increasing those computer and information resources skills crucial to education, research, and professional development is also authorized.

b. NPS restricts only those uses of its computing and information system resources that are clearly inappropriate in a taxpayer-supported institution, or which are clearly inconsistent with the professional standards expected of its faculty, staff, and students. In any instance involving a question as to whether a specific action or conduct is or was appropriate, the primary consideration should be whether such action or conduct would be consistent with that expected of military officers, scholars, public servants, and members of the professional academic community, who realize that their actions reflect not only on themselves, but on NPS and DoD as well.

c. Network monitoring tools are used to obtain detailed information relating to network performance, security vulnerabilities, and the amount and types of usage. This information can be used to monitor compliance with School policies, including appropriate use. All users should be aware that NPS computer and information systems and networks are subject to monitoring at all times, and that use of these resources implies consent to such monitoring. Consequently, no

NAVPGSCOLINST 5230.4C

expectation of privacy should be assumed regarding information transmitted, received, or placed in NPS systems. Violations of the policies defined herein may subject the user to disciplinary action.

## 6. Specific Restrictions and Limitations

a. General. While individual computer system administrators normally define the parameters for use of their respective systems, there are certain activities so clearly not in keeping with the NPS mission or its status as a professional graduate school that they are expressly prohibited on all systems to which this policy applies. These are:

(1) Illegal, fraudulent, or malicious activities; partisan political activity; political or religious lobbying or proselytizing; or activities on behalf of organizations having no acknowledged affiliation with NPS; or, activities which result, or might reasonably be expected to result, in an allegation of harassment of an individual or group, regardless of their affiliation with NPS.

(2) Activities for the purpose of personal or commercial financial gain. This includes solicitation of business, services, or commercial products; conduct whose purpose is to further or support these activities.

(3) The use of any NPS computing resource for the purpose of transmitting or displaying inappropriate, offensive, or obscene language or material such as pornography, racial or ethnic slurs, personal insults, "hate literature", etc.; accessing, downloading, or storing files or material of a similar nature.

(4) Storing or processing classified information on any system not explicitly approved for classified processing.

(5) Using another individual's account or identity without their explicit permission.

(6) Viewing, modifying, or deleting other users' files or communications without appropriate authorization or permission.

NAVPGSCOLINST 5230.4C

(7) Activity for the purpose of circumventing or defeating the security or auditing functions of any system; surreptitious probing or examining of any system for the purpose of penetrating or disclosing security vulnerabilities of that system; or, the use of any program or utility for the purpose of conducting such activity, except as may be specifically authorized by the Superintendent, and only as part of legitimate system testing, security research, or in the performance of assigned security-related duties.

(8) Obtaining, installing, storing, or using software obtained in violation of the appropriate software license or copyright, or allowing unauthorized individuals to access or use NPS-licensed software in violation of the licensing agreement (i.e., software "piracy").

(9) Modifying or altering the operating system or configuration of any NPS system, including the installation of software, without first obtaining permission from the custodian or administrator of that system.

(10) Disclosing User IDs and Passwords, or otherwise permitting or enabling any unauthorized individual to access an NPS system.

(11) Storing, processing or displaying Sensitive Unclassified information, such as Privacy Act information or For Official Use Only, on systems which do not provide the appropriate protection for such material, or failing to adequately and prudently protect such material when it is stored, processed or displayed on appropriate systems.

b. There are certain other activities, which while not absolutely prohibited, are almost always inappropriate. Individuals engaging in them may be asked to justify their activities, and if reasonable justification does not exist may find their judgement and/or professional standards seriously questioned. Examples of such generally inappropriate activities are:

(1) Use of NPS systems that, in the judgement of the responsible system administrator, seriously interfere with other, legitimate uses or users. Examples include "hogging" systems for non-academic purposes (e.g., game playing); excessive large file transfers; excessive personal e-mail;

excessive storage of large (e.g., multi-media) files; storage of non-academic files, etc.

(2) Inconsiderate conduct toward other system users.

(3) Storing files or material that could be used for illegal or fraudulent purposes.

b. Web Pages. In addition to the general prohibitions cited above, the following policies specific to Web pages are also established:

(1) NPS Web servers may only be used for official business, and in an official capacity.

(2) Personal Web sites hosted by commercial Internet Service Providers (ISPs) will not be used for official purposes.

c. E-Mail. E-Mail originating from NPS systems establishes the sender's affiliation with NPS and the DoN/DoD. For this reason, such communications may be construed as being official in nature, or expressing official NPS or DoN/DoD policies or views. Users should also be aware of the capacity for their communications to reach a mass, even global, audience, or to be forwarded to unintended recipients. Users are expected to exercise appropriate discretion in the use of e-mail on NPS systems, in accordance with the following guidelines:

(1) E-mail will not be used to circumvent or bypass the normal chain of command for official actions.

(2) Originating, broadcasting or forwarding of chain letters or unsubstantiated security or virus alerts is prohibited.

(3) E-mail attachments should be scanned for viruses before transmission.

(4) The use of mass-mailing (defined as having 25 or more addressees) to multiple curriculums or departments on campus is authorized provided the subject matter reasonably relates to the legitimate academic or professional interests of the target audience, and is approved by the responsible

NAVPGSCOLINST 5230.4C

curricular officer or department head; mass-mailings off campus must be approved by the Superintendent or his designated authority.

(5) E-mail to bulletin boards, discussion groups or other subscription lists is exempt from specific approval provided users generally limit such participation to forums related to their own academic or professional expertise, and ensure their contributions are restrained, professional, objective, and clearly identified as personal opinions, rather than those representing official NPS or DoN/DoD views.

(6) The use of e-mail to initiate or conduct surveys may be authorized provided the surveys are conducted in accordance with reference (b) or (c), as applicable, and adhere to the guidelines set forth in this instruction; all surveys originating at NPS are subject to review by the NPS Staff Judge Advocate.

## 7. Responsibilities

a. Department heads, managers, and supervisors have the primary responsibility for implementation of these policies, and for ensuring that:

(1) This instruction receives appropriate dissemination, and that personnel under their authority are familiar with these policies, and that these policies are enforced within their respective departments and work centers.

(2) Appropriate mechanisms for reporting violations are implemented, and that the Command Information Systems Security Manager (ISSM), Code 005, is advised of any alleged violations.

b. Users of NPS computer and information systems are responsible for compliance with these policies, and reporting suspected or alleged violations via their chain of command.

8. Action. Maximum use will be made of available mechanisms for electronic distribution of this instruction within each department. Time lines for actions to be completed are as follows:

a. Within 45 days of the date of this instruction Line Managers and Department Heads will:

(1) Ensure that all NPS faculty, staff, and/or students under their authority read this instruction, and sign an acknowledgement that they understand and will comply with the policies set forth.

(2) Develop and implement procedures to ensure all new faculty, staff, and students, etc., are briefed on these policies, and sign an acknowledgement, before being granted access to any NPS or network resource to which this instruction applies.

(3) Ensure that student and faculty handbooks, user manuals, and standard operating procedures, etc., are updated, as appropriate, to reflect these policies.

b. Within 60 days of the date of this instruction, and annually thereafter, the NPS Information Systems Security Manager will verify that all departments have completed the actions specified, and submit a report of findings to the Superintendent.

ROGER L. BUSCHMANN  
By direction

Distribution:  
NAVPGSCOLINST 5605.2S (List 1)

